Simpson Thacher

Regulatory and Enforcement Alert

Key Takeaways From Recent SEC Cybersecurity Charges Against Advisers and Broker-Dealers

September 2, 2021

On August 30, 2021, the SEC announced three settlements with eight registered investment advisers and broker-dealers for violations of Rule 30(a) of Regulation S-P (the "**Safeguards Rule**") and, in the case of one of the firms charged, for violations of Section 206(4) and Rule 206(4)-7 of the Advisers Act, resulting in hundreds of thousands of dollars in fines (ranging from $200,000 to $300,000) for the firms. The settlements reflect the Enforcement Division's continued focus (for issuers and advisers alike) on cybersecurity, as well as a continued focus on advisers' adherence to adopted policies and procedures. These actions originated in examinations and may reflect the developed expertise of the Exams Staff (working with the SEC's specialized Cyber Unit) on cybersecurity issues.

The settlements come on the heels of a number of initiatives and publications by the SEC with respect to cybersecurity risks.[1] In its 2021 Examination Priorities, the Division of Examinations ("**Examinations**") noted that it "will also focus on controls surrounding . . . the electronic storage of books and records and personally identifiable information maintained with third-party cloud service providers, and firms' policies and procedures to protect investor records and information." Examinations also published a January 2020 report regarding effective cybersecurity practices for market participants, as well as a COVID-related risk alert in August 2020 that included focus on cyber risks.

Both registered investment advisers and broker-dealers should be mindful that they are expected to take a proactive approach to addressing cybersecurity challenges and should periodically assess the effectiveness of their policies and procedures as their practices and available technology solutions evolve over time.

Settlements

The three settlements involved eight firms: Cetera Advisor Networks LLC (a dually registered broker-dealer and investment adviser), Cetera Advisors LLC (a dually registered broker-dealer and investment adviser), Cetera Investment Services LLC (a dually registered broker-dealer and investment adviser), Cetera Financial Specialists LLC (a registered broker-dealer) and Cetera Investment Advisers LLC (a registered investment adviser) (together, "**Cetera**"); Cambridge Investment Research, Inc. (a registered broker-dealer) and Cambridge Investment

[1] These initiatives also include developments for corporate issuers, including proposed rule changes for public companies with respect to their cybersecurity disclosures.

Research Advisors, Inc. (a registered investment adviser) (together, "**Cambridge**"); and KMS Financial Services, Inc. (a dually-registered broker dealer and investment adviser) ("**KMS**"). Each of the firms experienced compromises of its email accounts (many of which were maintained on cloud-based systems) that arose from alleged failures or lapses in their cybersecurity policies and procedures. As a result, personally identifying information ("**PII**") from thousands of customers and clients of these firms was exposed to hackers and otherwise put at risk.

Each of the firms were charged with violations of the Safeguards Rule, which requires broker-dealers, investment companies and investment advisers registered with the SEC to "adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." The Safeguards Rule further mandates that these policies and procedures should be designed to (1) insure the security and confidentiality of customer records, (2) protect against anticipated threats or hazards to security or integrity of such records and (3) protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to customers. The orders each emphasize that the firms did not take advantage of existing technology tools available to them and that the SEC seems to suggest may be warranted, particularly where the firms were using cloud-based systems to store email. For example, each of the orders stresses that firms did not use multi-factor authentication ("**MFA**") technology that was available to them to secure some or all of their systems, despite policies that strongly encouraged use of such technology (in the case of Cetera) or recommendations by cybersecurity consultants (in the case of KMS). For each of the firms, failure to detect breaches and subsequent failures to implement additional cybersecurity features following initial breaches may have contributed to additional breaches or cybersecurity lapses, and such delays continued to place customer information at risk since the takeovers each occurred over a number of quarters or years.

In the case of Cetera, the SEC also alleged violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 promulgated thereunder, which require advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act. The SEC found that Cetera failed to modify disclosures to customers whose information was exposed, stating in communications to affected customers that incidents occurred two months earlier when in actuality such events had occurred up to six months earlier. These misstatements—which the SEC notes may have been the result of oversight in adjusting template notification language—was misleading because customers may not have been aware that the exposure could have had effects on their information prior to the stated date of the incidents and further was in violation of Cetera's policies and procedures that required firm personnel to review client communications for cybersecurity incidents for accuracy before they were distributed. Cetera was expected to have sufficient policies and procedures in place to ensure that such errors in communications were detected before distributed to customers. Notably, despite these communications relating to disclosure issues, the SEC did not allege violations of Section 206(2) of the Advisers Act.

Takeaways

The Staff has emphasized that these cybersecurity cases involve failures by advisers and broker dealers to "fulfill their obligations concerning the protection of customer information." Most notably, the action involving Cetera appears to signal that the SEC will evaluate cybersecurity incidents and related disclosures to impacted parties not only in terms of the Safeguard Rule but also with respect to an adviser's obligations to maintain and enforce policies and procedures reasonably designed to prevent violations of the Advisers Act under Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder. The settlement involving Cetera, in particular, indicates that Enforcement may be open to pursuing more novel enforcement theories based on a firm's response to a cybersecurity matter, enhancing the importance of firms to "get-it-right" even when they themselves (and their personnel) may be victims of these cyber-attacks.

Advisers and broker-dealers should ensure that they are regularly reviewing (and testing) their cybersecurity policies and procedures with input from their internal and external information technology and cybersecurity advisors. Importantly, firms must ensure that they are enforcing existing cyber policies and procedures across the entire firm (including consultants and temporary employees who may have access to—or whose credentials may be used to access—confidential customer information such as PII). The orders make it evident that the SEC will evaluate whether technology was reasonably available to firms in assessing their compliance with the Safeguards Rule and will question whether a recommended and available technology solution (such as adoption of MFA) should have been mandatory in order to reasonably prevent cybersecurity failures.

Finally, firms should be prepared for how they will respond to a cyber-attack, including identifying key respondents, conducting tabletop exercises and making sure that policies and procedures are in place (and followed) to respond timely and accurately. And, of course, as the Cetera order makes clear, accuracy in external communications to customers impacted by cyber incidents is crucial.

CONTACT THE AUTHORS

For further information about this Alert, please contact the following authors: Marc P. Berger, Stephen M. Cutler, Nicholas S. Goldin, Meaghan A. Kelly, Michael J. Osnato, Jr., Allison Scher Bernbach, William LeBas or any other member of the **Funds Regulatory and Investigations** Group or **Privacy and Cybersecurity** Practice below.

FUNDS REGULATORY AND INVESTIGATIONS GROUP/PRIVACY AND CYBERSECURITY PRACTICE

Martin S. Bell
+1-212-455-2542
martin.bell@stblaw.com

Rajib Chanda
+1-202-636-5543
rajib.chanda@stblaw.com

Stephen M. Cutler
+1-212-455-2773
stephen.cutler@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Joshua A. Levine
+1-212-455-7694
jlevine@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

Allison Scher Bernbach
+1-212-455-3833
allison.bernbach@stblaw.com

Marc P. Berger
+1-212-455-2197
marc.berger@stblaw.com

Brooke E. Cucinella
+1-212-455-3070
brooke.cucinella@stblaw.com

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

Meaghan A. Kelly
+1-202-636-5542
mkelly@stblaw.com

Owen Lysak
+44-(0)20-7275-6179
owen.lysak@stblaw.com

Michael W. Wolitzer
+1-212-455-7440
mwolitzer@stblaw.com

William LeBas
+1-212-455-2617
william.lebas@stblaw.com

David W. Blass
+1-202-636-5863
david.blass@stblaw.com

Paul C. Curnin
+1-212-455-2519
pcurnin@stblaw.com

Adam Goldberg
+852-2514-7552
adam.goldberg@stblaw.com

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Keith A. Noreika
+1-202-636-5864
keith.noreika@stblaw.com

Jonathan K. Youngwood
+1-212-455-3539
jyoungwood@stblaw.com